J. nr. 12-10153

SIKKERHEDSPOLITIK FOR DANSK AUTOGENBRUG

1. INDLEDNING

Sikkerhedspolitikken skal til enhver tid understøtte virksomhedens værdigrundlag og vision samt demonstrere, at virksomheden har en seriøs holdning til sikkerhed for persondata, systemer og andre IT-aktiver.

Hensigten med sikkerhedspolitikken er endvidere at tilkendegive over for alle, som har en relation til virksomhed, at anvendelse af informationer og informationssystemer er underkastet standarder og retningslinjer.

Fastholdelse og udbygning af et højt sikkerhedsniveau er en væsentlig forudsætning for, at virksomheden fremstår troværdig, og for at fastholde denne troværdighed skal det sikres, at al information behandles med fornøden fortrolighed og at der sker fuldstændig, nøjagtig og rettidig behandling af godkendte transaktioner.

IT-systemer betragtes, næst efter medarbejderne, som virksomhedens mest kritiske ressource. Der lægges derfor vægt på driftsikkerhed, kvalitet, overholdelse af lovgivningskrav og på at systemerne er brugervenlige, dvs. uden unødigt besværlige sikkerhedsforanstaltninger.

Der skal skabes et effektivt værn mod IT-sikkerhedsmæssige trusler, således at vores image og medarbejdernes tryghed og arbejdsvilkår sikres bedst muligt. Beskyttelsen skal være vendt imod såvel naturgivne som tekniske og menneskeskabte trusler. Alle personer betragtes som værende mulig årsag til brud på sikkerheden; dvs. at ingen persongruppe skal være hævet over sikkerhedsbestemmelserne.

Tilsidesættelse af denne IT-politik kan få aftaleretlige, herunder ansættelsesretlige, konsekvenser for såvel medarbejdere, ledelse som leverandører. Ledelsen er pligtig at påse overholdelsen.

Denne politik er udarbejdet på et tidspunkt, hvor der alene er ansat en direktør og en freelance-bogholder i virksomheden.

2. FORMÅL

Målene for virksomhedens sikkerhedspolitik er at

- opnå høj driftsikkerhed med høje oppetidsprocenter og minimeret risiko for større nedbrud og datatab - TILGÆNGELIGHED
- opnå korrekt funktion af systemerne med minimeret risiko for manipulation af og fejl i såvel data som systemer - INTEGRITET
- opnå fortrolig behandling, transmission og opbevaring af data - FORTROLIGHED
- opnå en gensidig sikkerhed omkring de involverede parter - AUTENTICITET
- opnå en sikkerhed for gensidig og dokumenterbar kontakt - UAFVISELIGHED

alt under skyldig hensyntagen til den til enhver tid værende persondatalovgivning.

3. VIGTIGE GRUNDPRINCIPPER

3.1 FUNKTIONSADSKILLELSE

Funktionsadskillelse er det bærende kontrolprincip på såvel personligt som organisationsplan. Dette er sjældent praktisk fuldt ud muligt, blandt andet af hensyn til medarbejderens IT-færdigheder og -kompetencer. I det omfang, det er muligt, og opgaven således ikke er outsourcet til en databehandler, herunder et lønbureau eller en IT-supporteringsvirksomhed, er det ledelsens pligt at sikre, at alle nødvendige behandlingsskridt noteres med navn, dato og beskrivelse af behandlingen.

3.2 SIKKERHEDSFORANSTALTNINGER

Ledelsen beslutter omfang og styrke af de sikkerhedsforanstaltning, der findes nødvendige at installere. Sådanne installeres af den IT-ansvarlige, hvilken funktion kan være outsourcet. Ledelsen varetager og formulerer administrative foranstaltninger ved nye tiltag og foranstaltninger, herunder udarbejdelse af retningslinjer og instrukser.

3.3 STYRING AF SIKKERHEDSHÆNDELSER

Ledelsen skal løbende sikre og monitere eventuelle hændelser, der kan true sikkerheden, således at risikoen for databrud kan minimeres eller undgås.

Ledelsen er opmærksom på pligten til at foretage indberetning af databrud. Ved databrud skal følgende iagttages: Virksomheden skal foretage anmeldelse af sikkerhedsbruddet til Datatilsynet uden unødig forsinkelse, dog senest 72 timer efter, vi er blevet bekendt med bruddet.

Anmeldelsen skal foretages af direktøren som kontaktperson, og anmeldelsen skal mindst

- beskrive karakteren af bruddet, herunder forventet antal berørte og kategorierne af oplysninger,
- sandsynlige konsekvenser af sikkerhedsbruddet, og
- de foretagne foranstaltninger, der er truffet.

Derudover dokumenterer ledelsen alle brud på persondatasikkerheden, herunder de faktiske omstændigheder ved bruddet, dets virkninger og de trufne, afhjælpende foranstaltninger.

Hvis bruddet indebærer en høj risiko for fysiske personer, underretter vi som udgangspunkt den unødig forsinkelse de registrerede om bruddet. Ledelsen har ansvaret herfor.

3.4 DOKUMENTATION

Såfremt der skal udføres særlige, væsentlige sikkerhedsaktiviteter, skal disse planlægges, risikovurderes og dokumenteres.

4 ORGANISERING AF SIKKERHEDSARBEJDET

Ledelsen har det overordnede ansvar for sikkerhedsarbejdet, herunder det IT-mæssige. Ledelsen kan og skal i fornødent omfang inddrage samarbejdspartnere, der fungerer som databehandlere.

Ledelsen har ansvaret for udformningen af sikkerhedspolitikken, herunder opdateringer heraf, ligesom ledelsen udpeger den eller de personer, der skal have adgang til især følsomme persondata.

5 SIKKERHEDSBEVIDSTHED

Enhver person, der håndterer eller har adgang til persondata eller andet følsomt materiale underlagt denne sikkerhedspolitik skal være underlagt tavshedspligt i kontrakt.

6 STYRING AF AKTIVER

Virksomhedens IT-aktiver (software, data og fysiske enheder) skal identificeres og registreres med en ejer, der typisk vil være den daglige bruger heraf. Registreringen kan varetages af en ekstern samarbejdspartner. Er der tale om en hostet løsning, skal der tages hensyn hertil i aftalegrundlaget med samarbejdspartneren, afhængigt af, om vedkommende optræder som databehandler.

Den registrerede ejer af aktivet har ansvaret for

- at aktivet til stadighed ved placering, brug og forandring m.v. opfylder IT-politikken,
- at aktivet ikke udsættes for særlig risiko, eksempelvis særlig usikre offentlige netværk m.v.

- at aktivet til stadighed er forsynet med en af den registrerede ejer selvvalgt og hemmelig kode, der SKAL fornys mindst hver 3. måned eller med biometrisk lås, fx fingeraftryk,
- at aktivet til stadighed er forsynet med tilstrækkelig og opdateret firewall og viruskontrol. Ordinær opdatering af disse programmer foretages automatisk af ekstern leverandør. Ledelsen er opmærksom på, at telefoner og tablets umiddelbart er mere udsatte for sådanne risici end computere. Aktuelt vil der dog ikke blive lagt restriktioner på brugen af virksomhedens aktiver, ej heller i forhold til privat brug. Beslutning herom er truffet efter en konkret risiko-vurdering.
- at sensitive koder ikke lagres automatisk og programmer med følsomme data er selvstændigt kodet,

Ved oprettelse af forbindelse til usikre, typisk offentlige netværk uden adgangskode, må VPN-tunnellen ikke benyttes. Skal der oprettes forbindelse hertil, SKAL netværksforbindelse oprettes via en kodet, sikret forbindelse, fx via netværksdeling på egen mobiltelefon.

Ethvert aktiv skal sikre og beskyttes mod uautoriseret adgang, misbrug eller ødelæggelse under transport eller ved opbevaring. Dette gælder også – og især – bærbare computere, tablets og mobiltelefoner. Den enkelte registrerede ejer har ansvaret for aktivernes beskyttelse udenfor kontoret, herunder ved opbevaring i hjemmet.

Bortskaffelse af aktiver, som indeholder eller kan give adgang til persondata og andre følsomme oplysninger, herunder fortrolig information af hvad art tænkes kan, skal ske efter aftale med og instruks fra ledelsen, der skal sikre, at aktivet lagres og dokumenteres, hvorefter bortskaffelse kan ske forsvarligt, eksempelvis ved destruktion, makulering eller definitiv sletning af data.

Det er tilladt at benytte virksomhedens aktiver til privat brug.

7 STYRING AF ADGANG – ELEKTRONISK

Enhver elektronisk adgang til virksomhedens systemer kræver log-on-koder. Alle fysiske aktiver kræver korrekt indtastet kode indenfor 3 forsøg. Herefter blokeres der for adgang indtil direktøren har godkendt ny opsætning af adgang.

Forgæves log-on-forsøg med spærring registreres automatisk i IT-systemet.

Den selvvalgte kode skal som minimum bestå af 8 tegn, store og små bogstaver samt tal.

7.1 HR-OPLYSNINGER

Alle persondata, herunder følsomme, kan alene tilgås af bogholderen og direktøren, der har ansvaret for lønbogholderi henholdsvis virksomhedens daglige ledelse. Disse oplysninger kan alene tilgås af de pågældende efter indtastning af en af dem valgt kode til systemet.

7.2 KUNDE-/MEDLEMSDATA

Såvel direktøren som bogholderen har behov for persondata på medlemmer.

7.3 PRIVAT BRUG AF AKTIVER OG E-MAILS

Private e-mails skal være forsynet med emnefeltet "PRIVAT" og placeres i en selvstændig mappe af samme navn. Private e-mails skal slettes straks ved arbejdsforholdets ophør, såfremt medarbejderen ikke forud herfor selv har gjort dette. Virksomhedens sletteplig skal kun iagttages, såfremt mærkningen af e-mails er sket som anført.

8 STYRING AF ADGANG – FYSISK

Alle følsomme persondata opbevares i aflåste skabe. Almindelige oplysninger opbevares i ringbind på direktørens kontor på virksomhedens adresse. Virksomhedens lokaler låses af udenfor normal arbejdstid og er sikret eksternt med alarm og koder.

Alle fysiske dokumenter, der indeholder persondata, almindelige eller følsomme, skal opbevares utilgængelige for uvedkommende, herunder i skabe eller andre arkivalier, og sådanne skal makuleres, når disse ikke længere benyttes eller der foreligger en sletteplig i øvrigt iht. virksomhedens privatlivspolitik.

Når fysisk materiale, der indeholder persondata, skal slettes, sker dette ved makulering direkte på virksomhedens adresse. Virksomheden har en makuleringspolitik, hvorefter ikke kun materiale indeholdende persondata, men også andre kritiske oplysninger, herunder om samarbejdspartnere, økonomi m.v. skal makuleres.

9 E-MAIL- OG KOMMUNIKATIONSSIKKERHED

Ingen e-mails må indeholde persondata i emnefeltet, ligesom e-mail indeholdende følsomme persondata i videst muligt omfang skal fremsendes krypteret eller via e-boks. Lønsedler og andre HR-relaterede oplysninger skal altid fremsendes krypteret, kodet eller med sikker post.

Al overførsel af information, herunder via e-mail, skal klassificeres i forhold til persondatalovgivningen, ligesom der skal foretages en konkret risikovurdering. Om nødvendigt kan brugen af begrebet "fortroligt" eller "hemmeligt" benyttes i emnefeltet til forsendelse og overførsel.

E-mails skal sendes til og fra @autogenbrug.dk-domænet, således at alle e-mails kan spores og sletning alene skal foretages fra én mail-server. Ledelsen har noteret sig, at virksomheden ikke aktuelt har et fast system til kryptering af e-mails, men ledelsen observerer omfanget af behovet og træffer herudfra beslutning om, hvorvidt et sådant system skal erhverves.

10 DRIFTSSIKKERHED, ANSKAFFELSE OG VEDLIGEHOLDELSE

Driftssikkerhed drejer sig om at opnå korrekt og sikker drift af de faciliteter og systemer, der behandler, herunder opbevarer, information og persondata. Heri indgår dokumentation af procedurer for drift, softwareinstallation samt styring af ændringer, der løbende forekommer, herunder opdateringer, som kan påvirke sikkerheden.

Der skal indføres sikkerhedsforanstaltninger, der kan opdage og forhindre data- og sikkerhedsbrud, eksempelvis forårsaget af malware. Ligeledes skal der foretages løbende backup af data, ligesom der skal udarbejdes en backup-plan til brug for større sikkerhedsbrud.

Enhver anskaffelse med tilhørende installation og vedligeholdelse må alene ske fra en leverandør, der opfylder betingelserne i pkt. 11.

11 OUTSOURCING

Leverandører, der helt eller delvist står for drift af virksomhedens aktiver og systemer skal overholde virksomhedens IT-sikkerhedspolitik. Der skal være mulighed for at udøve effektiv kontrol hermed, ligesom leverandører skal kunne dokumentere deres overholdelse.

I forbindelse med outsourcing kan det blive nødvendigt at udarbejde en databehandleraftale, der i detaljer skal beskrive de sikkerhedskrav, som leverandøren skal leve op til.

12 VERSION OG OPDATERING

Den hurtige udvikling af internettet betyder, at ændringer i sikkerhedspolitikken kan blive nødvendige. Derfor kan og skal ledelsen foretage ændringer heri, såfremt det er nødvendigt. Enhver ændring skal meddeles de berørte pligtsubjekter, eksempelvis medarbejderne.

Denne sikkerhedspolitik er senest ændret den 19. juni 2018.